Cours 1 : Introduction à la cybersécurité et à la Directive NIS2

Cycle de webinaires - Renforcez la cybersécurité de votre organisation pour contrer les cyberattaques : règlementation et mise en pratique

Webinaire | Lundi 10 février 2025 | Belgique | Jeoffrey Vigneron

Description

Plongez au cœur de **la cybersécurité et de la conformité avec la nouvelle Directive NIS2** grâce à ce cycle de formations complet, réparti en trois webinaires interactifs. Accompagné d'experts chevronnés, vous explorerez les **fondations de la sécurité numérique, les cadres de conformité et de bonnes pratiques, ainsi que l'implémentation technique concrète** pour assurer la résilience de votre organisation.

Pourquoi participer ?

- Maîtriser les **enjeux et la législation récente** : Découvrez l'impact et les obligations introduites par la Directive NIS2 (Directive (UE) 2022/2555) et apprenez à les mettre en œuvre
- **Approche opérationnelle** : Familiarisez-vous avec le CyberFundamentals Framework (CyFun), inspiré de standards internationaux (NIST CSF, ISO/IEC 27001, CIS Controls, IEC 62443), ainsi qu'avec les conditions d'application de l'ethical hacking
- **Mise en pratique immédiate** : Grâce à des études de cas, des exercices de simulation d'incidents et des checklists issues de l'expérience terrain, vous serez en mesure de concevoir et déployer des solutions concrètes, tout en vous appuyant sur des outils de référence
- **Adapté à votre contexte** : Qu'il s'agisse d'une PME, d'une organisation essentielle ou d'un prestataire de services, ce cycle vous guidera dans la mise en conformité légale, technique et organisationnelle
- **Garantir la résilience et la réputation de votre entité** : Anticipez les risques, réduisez votre surface d'attaque et protégez vos données sensibles pour maintenir la confiance de vos clients, de vos partenaires et des autorités de régulation (ex. Centre pour la Cybersécurité Belgique – CCB)

Ce que vous obtiendrez :

- Une vision claire de la cybersécurité moderne et de la Directive NIS2
- Des bases solides pour mettre en œuvre le CyberFundamentals Framework (CyFun)
- Des méthodes éprouvées pour planifier, exécuter et maintenir une stratégie de sécurité pérenne
- Un accompagnement pratique vers une conformité durable

Rejoignez-nous et faites de la cybersécurité un atout stratégique !

Ce même cycle sera proposé au mois de mars en anglais et sera prochainement annoncé.

Programme

1. Introduction

- 1.1. Objectifs du cours
  Comprendre les concepts fondamentaux de la cybersécurité et leur importance et découvrir la directive NIS2 et son impact sur les organisations.

- 1.2. Importance de la cybersécurité dans un monde connecté
  Chiffres récents sur les cyberattaques en Europe et exemples d'incidents majeurs ayant affecté des services critiques.

2. Cybersécurité : définition et enjeux

- 2.1. Définition et concepts-clés
  Cybersécurité, résilience, menaces, risques, incidents.

- 2.2. Principales menaces
  Phishing, ransomware, DDoS, attaques internes.

- 2.3. Bonnes pratiques
  Importance des sauvegardes, de la gestion des accès, des mises à jour régulières. Exemple : Analyse d'une cyberattaque récente en Belgique ou en Europe.

3. Présentation de la Directive NIS2

- 3.1. Objectifs et contexte
  Renforcer la résilience des infrastructures critiques et harmoniser les pratiques de cybersécurité dans l'UE.

- 3.2. Évolutions par rapport à NIS1
  Élargissement du champ d'application et Introduction de responsabilités accrues pour les organes de direction.

- 3.3. Obligations principales
  Mesures organisationnelles et techniques - Notification des incidents de sécurité significatifs - Coopération avec les autorités nationales (CCB en Belgique). Exemple : Étude de cas : application de NIS2 dans le secteur de la santé.

4. Champ d'application et sanctions

- 4.1. Identification des entités concernées
  Différence entre entités essentielles (EE) et importantes (EI). Critères de classification (taille, criticité des services).

- 4.2. Régime de sanctions
  Amendes financières et impacts juridiques et réputationnels.

5. Processus de mise en conformité avec NIS2

- 5.1. Étapes vers la conformité
  Évaluation des risques - Planification des mesures correctives - Mise en œuvre des solutions.

- 5.2. Documentation et rapports
  Registre des actifs critiques - Rapports sur la gestion des risques - Communication avec les autorités. Exemple : Mise en conformité d'une PME fictive opérant dans le secteur des transports.

6. Conclusion et Q&A

Synthèse des points abordés et session interactive pour répondre aux questions.

Orateurs

- **Jeoffrey Vigneron** : Avocat au barreau de Bruxelles, coding lawyer et fondateur du cabinet lawgitech

Informations pratiques

Dates et horaire

Lundi 10 février 2025

De 14h00 à 17h00

Lundi 10 février : Cours 1 : Introduction à la cybersécurité et à la Directive NIS2

Lundi 17 février : Cours 2 : Introduction au CyberFundamentals Framework (CyFun) et ethical hacking

Jeudi 20 février : Cours 3 : Implémentation technique et cas pratiques

Lieu

En ligne

Vous pourrez suivre la formation en direct sur le Web. Vous recevrez les détails de connexion à l'avance par e-mail.

Attention ! L'adresse e-mail par laquelle vous procédez à l'inscription sera l'adresse à laquelle le lien vers le webinaire sera envoyé. Si vous vous inscrivez par l'intermédiaire d'une autre personne (secrétaire, collègue…), cette personne devra vous faire suivre le lien en question pour que vous puissiez vous connecter et suivre la formation. Les inscriptions qui arrivent moins d'une heure avant le début du webinaire ne seront malheureusement pas prises en compte.

Prix

230 € TTC - Participation à un cours

594 € TTC - Participation aux trois cours

Public visé

Ce cycle est proposé à tous les professionnels cherchant à renforcer leurs compétences en matière de cybersécurité, de conformité légale et de protection des systèmes d'informations et des données afin d'assurer la sécurité de leur organisation.

Le cycle peut également être tout autant bénéfique pour les avocats, notaires, huissiers de justice, les juristes d'entreprises, CISO, DPO, RSSI … qui sont chargés de traiter des questions technico-juridiques liées à la sécurité des données et à la conformité réglementaire et soucieux de se prémunir de toute cyberattaque pour leur organisation.

Formation permanente

Une demande d'agrément a été introduite auprès de AVOCATS.BE, avocats.lu, l'IJE et SAMTES

Ce webinaire peut faire l'objet d'une prime Liberform si vous remplissez les conditions.

Renseignements complémentaires

Larcier-Intersentia

formations@larcier-intersentia.com

Numéro gratuit : 0800 39 067